

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)
)
Modernization of the Nation’s Alerting) PS Docket No. 25-224
Systems)
)

**Comments of Sage Alerting Systems, Inc.
Regarding the Modernization of the Nation’s Alerting Systems NPRM**

September 25, 2025

1 Introduction

Sage Alerting Systems has been actively involved in the Emergency Alert System (EAS) since its inception 31 years ago. In much of our committee¹ participation, we have consistently highlighted the need for a comprehensive "why are we doing this" review of EAS, including an introspection into what is truly needed versus what is currently being implemented. We are pleased that the Commission has now formally initiated a process to address these critical questions.

We don’t presume to speak for originators, broadcasters, or the general public. Sage, as with many technologists, turns requirements into solutions, and we look forward to continuing to serve the community as it defines new goals and strategies.

In this document, we’ll discuss the major design constraint for the existing EAS system - its narrow audio bandwidth and resulting limited AFSK data rate. We’ll highlight that this feature enables the station to station relay component of EAS that gives EAS the ability to provide resilience to the larger warning system of which EAS is a part.

2 The Emergency Alert System’s Role in Emergency Notifications

In 1997, when EAS came into common use, it was the only mandated means of sending alerts for relay by an unattended, automated broadcaster. The primary purpose was for FEMA to issue Emergency Action notifications on behalf of the White House, using FEMA’s Primary Entry Point system. Local Public Safety officials could also originate alerts, either directly on VHF/UHF channels, or in partnership with a local Primary station. However, the main

¹ CSRIC subcommittees, FEMA NAC IPAWS subcommittee, various standards groups, and ECIG

originator of messages has been and remains the National Weather Service via the NOAA Weather Radio system.

The data formats and audio quality were limited by the narrow band audio used by FEMA, NWS, and AM radio. It was designed to permit phone quality (3kHz) to AM Radio (5kHz in common practice) audio. These unconditioned paths were limited to low data rates (about 65 characters per second) to improve the likelihood of reception under varying conditions. Alerts were audio-based, with simple, predefined text used for TV crawls. By 2012, FEMA's Integrated Public Alert and Warning System, based on CAP, added a central collection and distribution point for more complex messages, including free-form text for TV crawls and first-generation audio. The CMAS/WEA cell phone interface was added. The IPAWS repository of alerts could be accessed by other systems, including social media platforms.

EAS² is now just one part of a larger set of public alert and warning systems, each having its own set of strengths and weaknesses. The strength of EAS when transmitted over radio and TV is its cross-connected station to station relay. This allows it to bridge gaps between areas that have lost internet or cell towers and those that have not, providing crucial resilience. Use of redundant alert sources, such as IPAWS via satellite, use of public safety VHF/UHF repeaters, Sirius/XM for national alerts, and neighboring stations add additional resilience to the overall warning system.

While the information available from the automated EAS system can be limited, it will reach large areas and serve as a door bell that alerts the listener that a problem exists, giving them initial information and starting them on the path of finding out more by using whatever other sources of information are available, including tuning to broadcast news stations.

Note that EAS is only part of a total national public alert system. EAS itself will never meet all of the desires of a total modern system – but it adds a resilience component to an overall system. The fallback narrow band component of EAS is supplemented by the information available by CAP – when the internet connectivity is available – making it possible for EAS to use high-fidelity audio, multiple languages, photos, and video³.

Many of the limitations of broadcast EAS, such as lack of fine-grained geofencing, are inherent in the delivery mechanism, i.e., broadcast. Some limitations in presentation, when the internet is not available, are due to the low data rate used – this includes multiple languages and a limiting number of vertices for geofencing polygons⁴.

What is gained by these limitations is resiliency and simplicity. In 2025, EAS is not meant to be the primary method to receive ongoing news coverage – this is still best served by mobile phones, the local news station, streaming, social media, etc. EAS is the backup – useful on that bad day when power outages at cell towers and ISPs make the internet unavailable, and even some local TV and Radio sources have lost power. Radio signals from outside of the emergency

² We refer to EAS as the traditional Part 11-defined system. New broadcast technologies, such as ATSC 3.0 include emergency service capabilities and more refined methods of delivering emergency information; however, when meeting EAS requirements, they still use AFSK signaling and a text crawl.

³ When such information is provided by links in the CAP message that can be fetched at high speed.

⁴ Legacy EAS does not define a method of sending location polygons.

area, triggered by redundant local primary EAS stations, might still deliver an alert. That is EAS's contribution: it isn't "the" warning system but it is a resilient backup to the other warning sources.

An important question the FCC needs to address is whether or not there is still a use case for the fallback narrow band audio "legacy" EAS. Do we still want/need it? Might the populace be better served by a funded satellite delivery system at each EAS participant to receive high fidelity CAP messages when the internet is down?

Many other countries use CAP for their emergency systems, but they don't also relay data through broadcasters by using AFSK data on the main audio channel. Canada, for example, uses a redundant internet feed to distribute alert messages to Radio, TV, and Cable systems.⁵

Sage believes that there is a use for the legacy EAS system, but there is a cost, in particular when considering security, multi-lingual support, and text presentation.

3 Adding Security to Over-the-Air EAS

This section is intended to highlight topics for discussion, as this proceeding is not the place for a full technical specification.

The security of the existing narrow-band EAS AFSK relay system can be improved using standard proven techniques. The goal is to secure legacy EAS messages, assuring a message is from an authorized originator. Legacy EAS⁶ messages are generated by:

- NOAA Weather Radio transmitters. Many EAS state plans recommend monitoring NWR and relaying alerts from NWR.
- A PEP station in response to an initiation by FEMA.
- An EAS participant in response to a message received in the CAP format from IPAWS, or from a State-maintained CAP server, or from a CAP message originated by a state or local county directly to a Satellite Distribution or system ATSC stream.
- Directly by a public safety organization, often as a backup to IPAWS, and transmitted on a public safety radio system.
- Directly by a local primary station, usually for monthly test, but can be any alert.
- Directly by any local station, typically for a required weekly test, but can be any alert.

Adding security to EAS would require that each legacy message include a digital signature of some type. Relay of a legacy EAS message would require the retransmission of the incoming message and signature, but not the generation of a new signature.

The techniques for digitally signing messages are well known. A variant of "detached signature" is a likely technique, and has been used for private EAS systems.

⁵ The Canadian weather service does use the Specific Area Message Encoding (SAME) protocol, as does the NWS, but Broadcasters don't monitor that source, instead using only the CAP internet feeds. The Canadian NAAD system (similar to IPAWS) historically provided satellite feeds of the CAP data, but Ku service ended in 2019. C-band ended in March 2025 due to an aging satellite and low use of the non-internet feeds.

⁶ In this discussion, "legacy EAS" refers to the data formats and AFSK modulation standards embodied in the current Part 11.31.

There are a few major sources of limitations when discussing adding signatures to legacy EAS:

- 1) **Data Rate:** EAS is sent in the main audio channel of the EAS participant's broadcast. This design is a requirement of the PEP system – using AM radio stations as relays for the Emergency Action Notification. The data rate of 520.83 bps derives from a NOAA standard intended for use over phone lines. While a higher data rate could be used, loss due to noise would increase, requiring a more robust protocol with self-correction capabilities, adding additional overhead. An unavoidable consequence of digital signatures would be longer alert header bursts and thus longer interruption of program audio.
- 2) **Internet Independence:** As a major feature of legacy EAS is to work when the internet is unavailable, we'd like legacy EAS to work without requiring internet access at the time the message is received.
- 3) **Key management:** Some agency needs to vet originators and provide and maintain signing keys.

There are several available mitigations.

Reduce the size of the signature header by not including an entire certificate.

Instead, use a small fingerprint for a certificate that is stored in a signed file obtained from a trusted source containing all active legacy-signing certificates. That file can be periodically downloaded and kept up to date as needed on the local EAS device, and used to validate legacy alerts as needed. The signature header would consist of the signed digest of the legacy message, and the fingerprint.

Reduce the number of permitted originators. Most EAS participants don't originate messages. Most that do are local primary stations that originate monthly tests. While all EAS participants must generate a weekly test, there is no need to sign a weekly test as weekly tests are not relayed, and are not meant to include audio. Limiting the number of originators will reduce the key management problem.

The CAP message must contain an EAS signature header for retransmission.

Originators of CAP messages that are intended to produce legacy EAS messages must provide the EAS signature header in the CAP message – that is, they must produce the signed digest of the EAS message that would be derived from the CAP message. This is a straight-forward process, as the algorithm used to produce a legacy EAS message is already defined in the EGIC Implementation Guide, and the originator already has a signing cert for the CAP message. FEMA would define a new CAP parameter to contain the EAS signature. Any EAS device that receives the CAP message and generates a legacy EAS message would also send the signature header contained in the CAP message.

To achieve the desired security improvement, while retaining the ability to send EAS alerts over narrow AFSK with internet unavailable at the time of reception, the above mitigations can be applied, and

- 1) An agency, such as FEMA, must issue certificates for EAS participants that need to originate legacy alerts.

2) NOAA, as a major source of EAS alerts, must digitally sign legacy alerts sent from NWR. With the detached signature scheme, they will still send the ZCZC portion of the alert as they always have, but will also send the EAS signature header.

3) We accept a longer interruption on broadcast outlets for alerts that are not RWTs.

The larger question to be answered is, do we want to continue to permit broadcasters to originate EAS messages? We still need Monthly Tests, but if we want to be secure, they should be issued by an IPAWS approved public safety source.

Another mitigation, of course, is to limit EAS to internet or satellite delivered CAP messages.

Sage believes that a security overlay can be added to legacy EAS if desired. A strong argument can be made for either adding security to legacy EAS, or removing that capability and using CAP-only EAS.

Respectfully Submitted,

/s/

Harold Price

President, Sage Alerting Systems, Inc.